



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/091,479	03/07/2002	Eric Rescorla	730.39867X00	3321
22907 7590 01/11/2007 BANNER & WITCOFF 1001 G STREET N W SUITE 1100 WASHINGTON, DC 20001			EXAMINER WON, MICHAEL YOUNG	
			ART UNIT 2155	PAPER NUMBER
SHORTENED STATUTORY PERIOD OF RESPONSE			MAIL DATE	DELIVERY MODE
3 MONTHS			01/11/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary

Application No.

10/091,479

Applicant(s)

RESCORLA ET AL.

Examiner

Michael Y. Won

Art Unit

2155

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 17 November 2006.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 28-31, 34-54, 57-61, 64 and 65 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☐ Claim(s) _____ is/are rejected.
- 7) ☒ Claim(s) 55, 56, 62 and 63 is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____
- 4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____
- 5) ☐ Notice of Informal Patent Application
- 6) ☐ Other: _____

DETAILED ACTION

1. This action is in response to the amendment filed November 17, 2006.
2. Claims 28, 30-43-44, 46, 49, 50-59, and 61-64 have been amended.
3. Claims 28-31 and 34-65 have been examined and are pending with this action.
4. Claims 28, 44, 46, 49, 55, and 62 previously rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement, has been withdrawn based on the amendments.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter, which the applicant regards as his invention.

5. Claim 44 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claim 44 recites the limitation "the SSL client handshake" in line 7 of claim 44.

There is insufficient antecedent basis for this limitation in the claim.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

6. Claims 28-31, 34-36, 39-40, 42- 54, 57, 59-61 and 64 are rejected under 35 U.S.C. 103(a) as being unpatentable over Aziz et al. (US 6,643,701 B1) in view of Bruck et al. (US 6,691,165 B1).

INDEPENDENT:

As per **claim 28**, Aziz teaches a method for clustered Secure Sockets Layer (SSL) acceleration comprising the steps of:

establishing a communication path between a first node and a second node via a first relay of the cluster (see col.4, lines 49-51: "an intermediary computer ("a relay") through which all communications flow is disposed between the client and the server), wherein the communication path includes an SSL connection between the first node and the first SSL relay (see col.8, lines 19-22: "using SSL, this link is established following handshaking session");

transferring information between the first node and the first relay, wherein the transferred information relates to a communication from the first node to the second node (see col.7, line 65-col.7, line 5: "Once links 210 and 230 are established, the secure connection program of client 200 and the secure connection program of server

240 transfer information between client 200 and server 240 through relay 220”) and wherein the transferred information includes a full record (implicit: see col.8, lines 58-62); and

transferring the information between the first relay and the second node (see col.7, line 65-col.7, line 5: “Once links 210 and 230 are established, the secure connection program of client 200 and the secure connection program of server 240 transfer information between client 200 and server 240 through relay 220”).

Aziz does not explicitly teach of connecting at least two relays in a cluster; and clustering state information of the communication path when the record has been acknowledged by the second node, the clustering comprising sharing the state information between the first relay and at least a second relay of the relay cluster, wherein the second relay is capable of taking over the communication between the first and second node upon failure of the first relay.

Bruck teaches of connecting at least two relays in a cluster (see Fig.2, #200; Fig.17, #1704; col.5, lines 33-35 & 38-40: “The front-layer servers 200 will also be referred to as a server cluster or gateway”; and col.28, lines 17-20: “distributed server 1703 of a server cluster 1704”); and clustering state information of the communication path (see col.10, lines 9-18: “provides state sharing information among the all the machines in the cluster”; and col.24, lines 31-33 & lines 40-42) when the record has been acknowledged by the second node (see col.25, line 58-col.26, line 6), the clustering comprising sharing the state information between the first relay and at least a second relay of the relay cluster (see col.10, lines 9-18: “provides state sharing

information among the all the machines in the cluster”), wherein the second relay is capable of taking over the communication between the first and second node upon failure of the first relay (see col.2, lines 49-54: “when a server failure at either layer is detected, the system automatically shifts network traffic from the failed machine to one or more operational machines”; col.3, lines 37-44; and col.7, lines 45-49: “fail-over capability”).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to modify the system of Aziz in view of Bruck by implementing at least two relays in a cluster and clustering state information of the communication path so that the second relay is capable of taking over communication between the first and the second nodes upon failure of the first relay. One would be motivated to do so because Aziz teaches that more than one relay can be employed to expand the number of connections (see col.6, lines 1-2).

As per **claim 44**, Aziz teaches a system for clustered Secure Sockets Layer (SSL) acceleration comprising:

a first node (see Fig.2: #200, “Client”);

a second node (see Fig.2, #240: “Servers”); and

an SSL (see col.8, lines 19-22: “using SSL, this link is established following handshaking session”) relay for connecting the first node and the second node (see col.4, lines 49-51: “an intermediary computer (“a relay”) through which all communications flow is disposed between the client and the server), comprising:

a first SSL relay configured to cluster an SSL handshake following reception of the SSL client handshake from the first node (see col.6, lines 51-55: "relay 320 will also handle handshake session resumption sessions with the clients in addition to handling new handshake sessions".

Aziz does not explicitly teach of a cluster comprising:

a second relay configured to transmit an acknowledgement to the first relay after receiving update information from the first relay; and

wherein the first relay is further configured to transmit a handshake acknowledgement message to the first node following reception of the acknowledgement from the second relay.

Bruck teaches a second relay configured to transmit an acknowledgement to the first relay (see col.8, lines 48-52 and col.10, lines 14-18) after receiving update information from the first relay (see col.25, line 58-col.26, line 6 and col.27, lines 12-15); and

wherein the first relay is further configured to transmit a handshake acknowledgement message to the first node following reception of the acknowledgement from the second relay (see col.27, lines 12-15).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to modify the system of Aziz in view of Bruck by implementing a second relay configured to transmit an acknowledgement to the first relay after receiving update information from the first relay and wherein the first relay is further configured to transmit a handshake acknowledgement

message to the first node following reception of the acknowledgement from the second relay. One would be motivated to do so because Aziz teaches that more than one relay can be employed to expand the number of connections (see col.6, lines 1-2).

As per **claim 46**, Aziz teaches computer readable medium storing computer readable instructions that, when executed by a processor, performs a method comprising:

establishing a connection between a first node and a second node via a first SSL (see col.8, lines 19-22: "using SSL, this link is established following handshaking session") relay of an SSL relay cluster (see col.4, lines 49-51: "an intermediary computer ("a relay") through which all communications flow is disposed between the client and the server), wherein the connection includes an SSL connection between the first SSL relay and the first node (see col.8, lines 19-22: "using SSL, this link is established following handshaking session");

receiving a data communication from the first node (see col.7, line 65-col.7, line 5: "Once links 210 and 230 are established, the secure connection program of client 200 and the secure connection program of server 240 transfer information between client 200 and server 240 through relay 220"), wherein at least a portion of the data communication is structured as a record (implicit: see col.8, lines 58-62);

transmitting the data communication to the second node (see col.7, line 65-col.7, line 5: "Once links 210 and 230 are established, the secure connection program of client

200 and the secure connection program of server 240 transfer information between client 200 and server 240 through relay 220"); and

receiving a first acknowledgment from the second node, wherein the first acknowledgement acknowledges the record (see col.8, lines 56-58: "server 340 would acknowledge that the end-to-end security session should resume and create link 330").

Aziz does not explicitly teach of wherein said relay cluster comprises at least two interconnected relays; following reception of the first acknowledgment, clustering state information of the established connection with at least a second relay of the relay cluster; and

receiving a second acknowledgment from the at least second relay in the relay cluster confirming successful clustering.

Bruck teaches of wherein said relay cluster comprises at least two interconnected relays (see Fig.2, #200; Fig.17, #1704; col.5, lines 33-35 & 38-40: "The front-layer servers 200 will also be referred to as a server cluster or gateway"; and col.28, lines 17-20: "distributed server 1703 of a server cluster 1704"); following reception of the first acknowledgment (see col.25, line 58-col.26, line 6), clustering state information of the established connection with at least a second relay of the relay cluster (see col.10, lines 9-18: "provides state sharing information among the all the machines in the cluster"; and col.24, lines 31-33 & lines 40-42); and

receiving a second acknowledgment from the at least second relay in the relay cluster confirming successful clustering (see col.8, lines 48-52).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to modify the system of Aziz in view of Bruck by implementing at least two relays in a cluster and clustering state information of the communication path. One would be motivated to do so because Aziz teaches that more than one relay can be employed to expand the number of connections (see col.6, lines 1-2).

As per **claim 49**, Aziz teaches an SSL relay, the SSL relay connected in a cluster of SSL relays, comprising:

a first interface for transferring information between a first node and the SSL relay (see col.4, lines 49-51: "an intermediary computer ("a relay") through which all communications flow is disposed between the client and the server), wherein the first interface includes an SSL connection between the first node and the SSL relay (see col.8, lines 19-22: "using SSL, this link is established following handshaking session") and wherein the information includes record formatted data (implicit: see col.8, lines 58-62);

a second interface for transferring information between a second node and the SSL relay (see col.7, line 65-col.7, line 5: "Once links 210 and 230 are established, the secure connection program of client 200 and the secure connection program of server 240 transfer information between client 200 and server 240 through relay 220");

Aziz does not explicitly teach of a third interface for transferring state information between relays in the cluster when the record formatted data has been acknowledged by the second node; and

a storage device, wherein state information of a connection between the first node and the relay is shared across each relay in the cluster, any of the relays in the cluster capable of taking over all connections of another relay in the cluster, wherein the storage device is further configured to store the transferred information in a queue until acknowledgment is received from the second node.

Bruck teaches of a third interface for transferring state information between relays in the cluster (see col.10, lines 9-18: "provides state sharing information among the all the machines in the cluster"; and col.24, lines 31-33 & lines 40-42) when the record formatted data has been acknowledged by the second node (see col.25, line 58- col.26, line 6); and

a storage device, wherein state information of a connection between the first node and the relay is shared across each relay in the cluster (see col.10, lines 9-18: "provides state sharing information among the all the machines in the cluster"), any of the relays in the cluster capable of taking over all connections of another relay in the cluster (see col.2, lines 49-54: "when a server failure at either layer is detected, the system automatically shifts network traffic from the failed machine to one or more operational machines"; col.3, lines 37-44; and col.7, lines 45-49: "fail-over capability"), wherein the storage device is further configured to store the transferred information in a queue until acknowledgment is received from the second node (see col.32, lines 34-36: "cache the assignment data").

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to modify the system of Aziz in view of Bruck by implementing a

third interface for transferring state information between relays in the cluster and a storage device wherein state information of a connection between the first node and the relay is shared across each relay in the cluster so that the second relay is capable of taking over communication between the first and the second nodes upon failure of the first relay. One would be motivated to do so because Aziz teaches that more than one relay can be employed to expand the number of connections (see col.6, lines 1-2).

DEPENDENT:

As per **claims 29, 45, 48, and 50**, which depend on claims 28, 44, 46, 49, respectively, Aziz further teaches wherein the first node comprises a client and the second node comprises a server (see Fig.2).

As per **claim 30**, which depends on claim 28, Aziz does not explicitly teach of further comprising transferring information related to communications between the first node and the second node to the second relay transparently upon failure of the first relay.

Bruck teaches transferring information related to communications between the first node and the second node to the second relay transparently upon failure of the first relay (see col.2, lines 49-54 & 63-65 and col.8, lines 62-65).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to modify the system of Aziz in view of Bruck by implementing transferring information related to communications between the first node and the second node to the second relay transparently upon failure of the first relay. One would

be motivated to do so because Aziz teaches that more than one relay can be employed to expand the number of connections (see col.6, lines 1-2).

As per **claim 31**, which depends on claim 28, Aziz teaches of further comprising transmitting the communication from the first node to a second SSL relay and from the second SSL relay to the second node (see Fig.3). Aziz does not explicitly teach of transmitting transparently upon failure of the first SSL relay.

Bruck teaches of transmitting transparently upon failure of the first SSL relay (see claim 28 and 30 rejections above).

As per **claim 34**, which depends on claim 28, Aziz does not explicitly teach of further comprising sharing a session cache across all of the at least two relays.

Bruck teaches of sharing a session cache across all of the at least two relays (see col.16, line 66-col.17, line 6).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to modify the system of Aziz in view of Bruck by implementing sharing a session cache across all of the at least two relays. One would be motivated to do so because Aziz teaches that more than one relay can be employed to expand the number of connections (see col.6, lines 1-2).

As per **claim 35**, which depends on claim 28, Aziz teaches of further comprising clustering an SSL session resumption between the first node and the one of the at least two SSL relays (see col.6, lines 51-55).

As per **claim 36**, which depends on claim 28, although Aziz teaches of further comprising cryptographic keying information (see col.8, lines 12-15), Aziz does not

explicitly teach of clustering across all of the at least two SSL relays (see col.13, lines 40-44).

Bruck teaches of clustering across all of the at least two SSL relays (see col.13, lines 40-44).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to modify the system of Aziz in view of Bruck by implementing clustering across all of the at least two SSL relays. One would be motivated to do so because Aziz teaches that more than one relay can be employed to expand the number of connections (see col.6, lines 1-2).

As per **claim 39**, which depends on claim 36, Aziz teaches of further comprising clustering a current key schedule (see col.8, lines 12-15).

As per **claim 40**, which depends on claim 36, Aziz teaches of further comprising clustering a key and an offset into a key stream (implicit: see col.8, lines 12-15).

As per **claim 42**, which depends on claim 28, Aziz teaches of further comprising clustering data from a partial record corresponding to data from either the first or second node (see col.7, lines 58-62).

As per **claim 43**, which depends on claim 28, Aziz teaches of further comprising clustering an information size (see col.8, lines 28-32).

As per **claim 47**, which depends on claim 46, Aziz does not teach wherein the second relay assumes the first relay's responsibilities upon failure of the first relay.

Bruck teaches wherein the second relay assumes the first relay's responsibilities upon failure of the first relay (see claim 30 rejection above).

As per **claims 51-54**, which depend on claim 49, Aziz further teaches wherein the first interface and the second interface and the third interface are the same (see col.6, lines 11-12).

As per **claims 57 and 64**, which depend on claim 28 and 46, respectively, Aziz teaches of further including the step of storing an unacknowledged portion of the information transferred between the first SSL relay and the second node in a queue (see col.12, lines 13-16).

As per **claim 59**, which depends on claim 44, Aziz further teaches wherein the update information includes at least one of: **a new TCP state, a current value of SSL handshake hashes and a handshake to enter upon failover.**

As per **claim 60**, which depends on claim 44, Aziz further teaches wherein the handshake acknowledgement message includes at least one of a server handshake and a server handshake completion message (see col.6, lines 51-55).

As per **claim 61**, which depends on claim 60, Aziz further teaches wherein the first node is configured to transmit a key exchange message once the server handshake completion message is received (see col.6, lines 51-55).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the

Art Unit: 2155

invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

7. Claims 37, 38, 41, 58 and 61 are rejected under 35 U.S.C. 103(a) as being unpatentable over Aziz et al. (US 6,643,701 B1) and Bruck et al. (US 6,691,165 B1), and further in view of Weinstein et al. (US 6,094,485 A).

As per **claim 37**, although Aziz and Bruck teaches of further comprising clustering a key (see claim 36 rejection above), Aziz and Bruck do not explicitly teach of clustering a current Cipher Block Chaining (CBC) residue.

Weinstein teaches of clustering a current Cipher Block Chaining (CBC) residue (see col.8, lines 5-10 and col.9, lines 24-28).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to modify the system of Aziz and Bruck in view of Weinstein by implementing clustering a current Cipher Block Chaining (CBC) residue. One would be motivated to do so because Aziz teaches of SSL (see col.8, lines 19-20) and that the relay is cleartext (see col.6, lines 61-62).

As per **claim 38**, Aziz and Bruck do not explicitly teach of further comprising clustering a sequence number.

Weinstein teaches of further comprising clustering a sequence number (see col.9, lines 29-34).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to modify the system of Aziz and Bruck in view of Weinstein by implementing clustering a sequence number. One would be motivated to do so

because Aziz teaches of SSL (see col.8, lines 19-20) and such implementation would provide a strong encryption scheme applicable with SSL.

As per **claim 41**, Aziz and Bruck do not explicitly teach of further comprising clustering a cipher state.

Weinstein teaches of clustering a cipher state (see col.11, lines 17-19).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to modify the system of Aziz and Bruck in view of Weinstein by implementing clustering a cipher state. One would be motivated to do so because such implementation would continue to provide transparent communication between the nodes even in the event of failure to one SSL relay.

As per **claims 58 and 65**, which depend on claim 57 and 64, respectively, although Aziz clearly suggests wherein the unacknowledged portion of the information transferred between the first SSL relay and the second node is stored in the queue (see claims 57 and 64 rejection above), Bruck does not explicitly teach of a cipher state associated with the information.

Weinstein teaches of cipher state associated with the information (see claim 41 rejection and motivation above).

Weinstein teaches of state information includes at least one of a chosen cipher suite (see col.1, lines 50-63).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to employ the teachings of Weinstein within the system of Bruck by implementing at least one of a chosen cipher suite within the system for clustered

Secure Sockets Layer (SSL) acceleration because such implementation would provide a strong encryption scheme applicable with SSL.

Allowable Subject Matter

8. Claims 55-56 and 62-63 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

The following is an examiner's statement of reasons for allowance:

The prior art of record does not disclose, teach, or suggest neither singly nor in combination the claimed limitation of "setting a timer when the record is read, wherein the record is a partial record; and clustering the partial record if the timer expires" as recited in claims 55 and 62.

As per claims 56 and 63, which depend on claim 55 and 62, respectively, prior art of record further does not disclose, teach, or suggest neither singly nor in combination the claimed limitation wherein the timer corresponds to two times a packet interval time.

Response to Arguments

9. Applicant's arguments with respect to claims 28-31 and 34-65 have been considered but are moot in view of the new ground(s) of rejection.

Applicant argues with respect to claims 28, 46 and 49 that Bruck fails to teach or suggest, "wherein the connection includes an SSL connection between the SSL relay and the first node".

Aziz et al. (US 6,643,701 B1) cited with the previous office action explicitly teaches of the above limitation (see rejection above).

Furthermore, with regards to the missing deficiency of an "SSL handshake", Aziz explicitly teaches this limitation.

Conclusion

9. For the reasons above claims 28-31 and 34-54, 57-61, 64, and 65 have been rejected and claims 55, 56, 62, and 63 have been objected. Claims 28-31 and 34-65 remain pending.

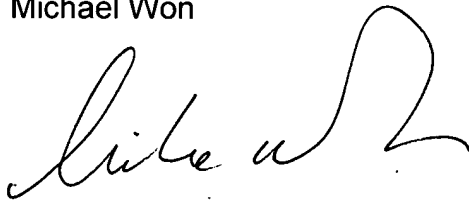
10. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Michael Y. Won whose telephone number is 571-272-3993. The examiner can normally be reached on M-Th: 7AM-5PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Saleh Najjar can be reached on 571-272-4006. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

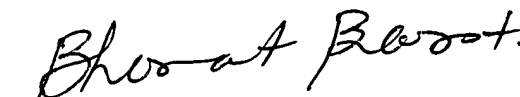
Art Unit: 2155

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Michael Won



December 28, 2006


BHARAT BAROT
PRIMARY EXAMINER